# Bussiness Impact Analysis Aplikasi Jaringan Komputer Dengan Teknik Packet Sniffing

**I Gede Putu Krisna Juliharta**
STMIK STIKOM Bali
Jl. Raya puputan Renon No. 86 Denpasar bali Telp (0361) 244445
e-mail: krisna@stikom-bali.ac.id

***Abstrak***

*Jaringan komputer sebagai jembatan tentunya banyak dilalui oleh data, dan besar kemungkinan di sadap untuk tujuan yang tidak baik sehingga bisa menyebabkan jaringan lumpuh, bisa juga menyebabkan pencurian data dari sebuah perusahaan. Dengan melakukan analisa jaringan menggunakan teknik packet sniffing diharapkan dapat menangkap data yang melalui jaringan. Data yang didapat diolah dan dikelompokkan menggunakan network miner. Hasil dari pengelompokan itu adaah IP address yang berkomunikasi. Setelah melakukan pengelompokkan dilanjutkan dengan penghitungan bussiness impact analysis dari IP address tersebut menggunakan perhitungan common vulnerability scoring system version 2 (CVSSv2) yang menghasilkan kelompok IP address dengan resiko high sebanyak 6 dan resiko medium sebanyak 9. Sehingga dapat disimpulkan pengelolaan jaringan selama ini sangat berisiko terhadap pencurian data.*

***Kata kunci:*** *jaringan, sniffing, IP address, Bussiness, Impact.*

***Abstract***

*Computer network as a bridge is of course passed by a lot of data, and there is a big chance can be tapped for bad purposes which can make the network to be paralyzed, it can also cause data theft of a certain company. By conducting network analysis using the sniffing packet technique, it is hoped to catch data which pass through the network. The data that are discovered then are processed and then categorized using the network miner. The result of that categorization is IP Address which communicate. After the categorization, it is then continued by counting the business impact analysis from that IP address using the calculation by the common vulnerability scoring system version 2 (CVSSv2) which results in IP Address Group with high risk in the amount of 6, and the IP Address Group with medium risk in the amount of 9. Thus it can concluded that the network management conducted is very risky to data theft.*

***Keywords****: network, sniffing, IP address, Bussiness, Impact.*

## 1. Introduction

Keruntuhan infrastruktur jaringan pada sistem jaringan merupakan bencana, menyebabkan terhentinya kegiatan sehari-hari suatu entitas karena kehilangan sumberdaya dan alat komunikasi. Masa fasilitas kemudahan berkomunukasi lenyap, dan peta jalan masa depan tiba tiba buram. Pertanggungjawaban menjadi tidak mungkin diberi atau diminta. bencana dapat menyebabkan infrastrukutur sistem yang telah dibangun hilang dalam waktu seketika.

Penerapan dari teknologi jaringan yang paling populer didunia adalah Internet. Penggunaannya sudah merambah semua kalangan, tua, muda, pribadi, perusahaan ataupun organisasi semuanya menggunakan internet. Teknologi yang awalnya digunakan untuk kebutuhan perang telah merambah dan menjadi tulang punggung kegiatan manusia dalam bekerja maupun gaya hidup. Ketergantungan terhadap teknologi informasi ini bukanlah tanpa resiko, banyak hal yang menyebabkan sistem bisa menjadi lumpuh. Lumpuhnya sistem tentunya mengakibatkan layanan terganggu.

Jaringan komputer sebagai jembatan tentunya banyak dilalui oleh data, dan besar kemungkinan di sadap untuk tujuan yang tidak baik sehingga bisa menyebabkan jaringan lumpuh, bisa juga menyebabkan tercurinya data dari sebuah perusahaan. Dengan melakukan analisa jaringan menggunakan teknik packet sniffing diharapkan dapat menangkap data yang melalui jaringan sehingga dapat dijadikan

bussiness impact analysis dari jaringan yang digunakan. Proses analysis menggunakan aplikasi wireshark dengan cara melakukan proses capture traffic yang melewati jaringan. Dari proses capture traffic tersebut dilanjutkan dengan mengelompokkan ip address yang berkomunikasi dengan menggunakan aplikasi network miner. Setelah menggunakan network miner dapat terlihat IP address yang sedang berkomunikasi dan protokol apa saja yang digunakan.

Hasil dari proses menggunakan wireshark dan network miner dilanjutkan dengan penghitunga bussiness impact analysis. Penghitungan ini menggunakan penilaian berbasis common vulnerability scoring system version 2 (CVSSv2). CVSS menghasilkan perhitungan resiko berdasarkan kerentanan yang dimiliki dalam proses komunikasi data. Network miner menghasilkan perangkat yang berkomunikasi pada saat proses capture berjalan, perangkat yang berdasarkan IP address tersebut, dilakukan analisa mengenai protokol yang digunakan dan pola komunikasi berjalan, hasil analisa dan pengelompokan IP dihitung kerentanan menggunakan CVSS sehingga menghasilkan tingkat resiko resiko dengan skala high, medium, dan low.

## 2. Landasan Teori

### 2.1 Jaringan Komputer

Jaringan komputer adalah kumpulan beberapa komputer yang saling terhubung satu sama lain melalui media perantara[2]. para ahli kemudian membagi jaringan komputer berdasarkan beberapa klasifikasi, Berdasarkan skala atau area, jaringan komputer dapat dibagi menjadi 4 jenis yaitu :

1. *Local Area Network* (LAN)
2. *Metropolitan Area Network* (MAN)
3. *Wide Area Network* (WAN)
4. *Internet*

Pengertian dari ke empat jenis diatas adalah sebagai berikut :

1. Local Area Network
   *Local Area Network* adalah jaringan lokal yang dibuat pada area tertutup. Misalkan dalam satu gedung atau dalam satu ruangan. Kadangkala jaringan lokal disebut juga jaringan privat. LAN biasa digunakan untuk jaringan kecil yang menggunakan *resource* bersama-sama, seperti penggunaan printer secara bersama, penggunaan media penyimpanan secara bersama.
2. *Metropolitan Area Network*
   *Metropolitan Area Network* menggunakan metode yang sama dengan LAN namun daerah cakupannya lebih luas. Daerah cakupan MAN bisa satu RW, beberapa kantor yang berada dalam komplek yang sama, satu kota, bahkan satu provinsi. Dapat dikatakan MAN merupakan pengembangan dari LAN.
3. *Wide Area Network*
   *Wide Area Network* cakupannya lebih luas daripada MAN. Cakupan WAN meliputi satu kawasan, satu negara, satu pulau, bahkan satu benua. Metode yang digunakan hampir sama dengan LAN dan MAN.
4. Internet
   Internet adalah interkoneksi jaringan-jaringan komputer yang ada di dunia. Sehingga cakupannya sudah mencapai satu planet, bahkan tidak menutup kemungkinan mencakup antar planet. Koneksi antar jaringan komputer dapat dilakukan berkat dukungan protokol yang khas, yaitu Internet Protocol (IP).

#### 2.1.1 Jaringan Berdasarkan Media Pengantar

Berdasarkan media penghantar, jaringan komputer dapat dibagi menjadi 2 jenis, yaitu :

1. *Wire Network*
   *Wire network* adalah jaringan komputer yang menggunakan kabel sebagai media penghantar. Jadi, data mengalir pada kabel. Kabel yang umum digunakan pada bahan dasar tembaga. Ada juga jenis kabel lain yang menggunakan bahan sejenis fiber optik atau serat optik. Biasanya bahan tembaga banyak digunakan pada LAN. Sedangkan untuk MAN dan WAN menggunakan gabungan kabel tembaga dan serat optik.
2. *Wireless Network*
   *Wireless network* adalah jaringan tanpa kabel yang menggunakan media penghantar gelombang radio atau cahaya infrared. Saat ini sudah semakin banyak outlet atau lokasi tertentu yang menyediakan layanan *wireless* network. Sehingga pengguna dapat dengan mudah melakukan akses internet tanpa kabel. Frekuensi yang digunakan pada radio jaringan komputer biasanya menggunakan frekuensi tinggi, yaitu 2,4 GHz dan 5,8 GHz. Sedangkan penggunaan infrared

umumnya hanya terbatas untuk jenis jaringan yang hanya melibatkan dua buah komputer saja atau disebut *point to point.* Hal ini menyebabkan infrared tidak sepopuler gelombang radio.

**2.1.2 Jaringan Berdasarkan Fungsinya**

Berdasarkan fungsinya, jaringan komputer dapat dibagi menjadi dua jenis, yaitu :

1. *Client Server*
   *Client server* adalah jaringan komputer yang salah satu (boleh lebih) komputer difungsikan sebagai server atau induk bagi komputer lain. Server melayani komputer lain yang disebut client. Layanan yang diberikan bisa berupa akses Web, E-Mail, File, atau lain sebagainya. Client Server banyak dipakai pada Internet. Namun LAN atau jaringan lain pun bisa mengimplementasikan client server. Hal ini sangat bergantung pada kebutuhan masing-masing.
2. *Peer to Peer*
   *Peer to Peer* adalah jaringan komputer dimana setiap komputer bisa menjadi server sekaligus client. Setiap komputer dapat menerima dan memberikan access dari/ke komputer lain. Peer to peer banyak diimplementasikan pada LAN. Walaupun dapat juga diimplementasikan pada MAN, WAN, atau Internet, namun hal ini kurang lazim. Salah satu alasannya adalah masalah manajemen dan security. Sulit sekali menjaga security pada jaringan Peer to Peer manakala pengguna komputer sudah sangat banyak.

**2.1.3 Web Serber**

Server web dapat merujuk baik pada perangkat keras ataupun perangkat lunak yang menyediakan layanan akses kepada pengguna melalui protokol komunikasi HTTP atau HTTPS atas berkas-berkas yang terdapat pada suatu situs web dalam layanan ke pengguna dengan menggunakan aplikasi tertentu seperti peramban web.

Penggunaan paling umum server web adalah untuk menempatkan situs web, namun pada prakteknya penggunaannya diperluas sebagai tempat peyimpanan data ataupun untuk menjalankan sejumlah aplikasi kelas bisnis.

Tahun 1989, Tim Berners-Lee mengajukan pada perusahaannya, CERN (European Organization for Nuclear Research) sebuah proyek yang bertujuan untuk mempermudah pertukaran informasi antar para peneliti dengan menggunakan sistem hiperteks. Sebagai hasil atas implementasi proyek ini, tahun 1990 Berners-Lee menulis dua program komputer:

sebuah peramban yang dinamainya sebagai World Wide Web;

server web pertama di dunia, yang kemudian dikenal sebagai CERN httpd, yang berjalan pada sistem operasi NeXTSTEP.

Dari tahun 1991 hingga 1994, kesederhanaan serta efektifitas atas teknologi yang digunakan untuk berkunjung serta bertukar data melalui World Wide Web membuat kedua aplikasi tersebut diadopsi pada sejumlah sistem operasi agar dapat digunakan oleh lebih banyak individu, ataupun kelompok. Awalnya adalah organisasi penelitian, kemudian berkembang dan digunakan di lingkungan pendidikan tinggi, dan akhirnya digunakan dalam industri bisnis.

Tahun 1994, Tim Berners-Lee memutuskan untuk membakukan organisasi World Wide Web Consortium (W3C) untuk mengatur pengembangan-pengembangan lanjut atas teknologi-teknologi terkait lainnya (HTTP, HTML, dan lain-lain) melalui proses standardisasi.

**2.1.4 Packet Sniffing**

Packet sniffing, network analyzers atau penyadapat paket merupakan sebuah proses untuk menangkap paket paket yang melintas melalui jaringan komputer. Untuk melakukan proses packet sniffing memerlukan aplikasi tertentu. aplikasi ini menangkap tiap-tiap paket dan kadang-kadang menguraikan isi dari RFC (*Request for Comments*) atau spesifikasi yang lain. Berdasarkan pada struktur jaringan (seperti hub atau switch), salah satu pihak dapat menyadap keseluruhan atau salah satu dari pembagian lalu lintas dari salah satu mesin di jaringan. Perangkat pengendali jaringan dapat pula diatur oleh aplikasi penyadap untuk bekerja dalam mode campur-aduk (*promiscuous mode*) untuk "mendengarkan" semuanya (umumnya pada jaringan kabel)[3].

Sniffer paket dapat dimanfaatkan untuk hal-hal berikut:

1. Mengatasi permasalahan pada jaringan komputer.
2. Mendeteksi adanya penyelundup dalam jaringan (*Network Intusion*).
3. Memonitor penggunaan jaringan dan menyaring isi isi tertentu.
4. Memata-matai pengguna jaringan lain dan mengumpulkan informasi pribadi yang dimilikanya (misalkan password).
5. Dapat digunakan untuk *Reverse Engineer* pada jaringan.

Untuk penelitian ini digunakan dua aplikasi untuk melakukan proses packet sniffing

**2.2 Commond Vulnerability Scoring System (CVSS)**

Dalam penjelasan yang diberikan oleh FIRST (*Forum Incident and Respond Team*) pada situsnya, *Common Vulnerability Scoreing System* (CVSS) merupakan standar industri terbuka yang dirancang untuk menyampaikan keparahan kerentanan dan membantu menentukan urgensi dan prioritas respon. CVSS dapat memecahkan masalah dari beberapa sistem penilaian yang tidak kompatibel dan dapat digunakan dan dimengerti oleh siapa saja.

CVSS telah digunakan oleh *Department of Homeland Security United state of America* dan terus mendorong penggunaan CVSS secara luas, dan dapat digunakan dengan sukarela. Banyak organisasi memiliki CVSS seperti Akamai, American Air, Symantec, Uni Pasifik dan organisasi lainnya CERT / CC, Cisco, HP, IBM, NIST, Oracle, Qualys, US-CERT[5].

Model CVSS dirancang untuk memberikan pengguna tentang nilai komposit yang mewakili keseluruhan tingkat keparahan dan risiko kerentanan (*risk of vulnerability*). Hal ini berasal dari metrik dan formula. Metrik yang berada di tiga kategori berbeda yang dapat secara kuantitatif atau kualitatif diukur. Base matrics mengandung kualitas yang intrinsik untuk setiap kerentanan diberikan yang tidak berubah dari waktu ke waktu atau dalam lingkungan yang berbeda. Temporal matrics mengandung karakteristik dari kerentanan yang berkembang selama masa kerentanan. Environment matrics Lingkungan mengandung karakteristik dari kerentanan yang terkait dengan implementasi di lingkungan pengguna tertentu.

Ada 6 parameter yang mendasari pembentukan sebuah base matrics, hal ini lah yang digunakan untuk tingkat *vulnerability* suatu sistem. Parameter tersebut adalah :

1. *Access Vector (AV)* mengukur seberapa jauh seorang penyerang dapat menyerang target.
    a. *Local*: Pemanfaatan kerentanan membutuhkan akses fisik ke target atau account (*shell*) lokal pada target.
    b. *Adjacent Network* (Jaringan Berdekatan): Pemanfaatan kerentanan membutuhkan akses ke jaringan lokal target.
    c. *Network* : kerentanan ini dieksploitasi dari jaringan remote.
2. *Access Complexity (AC)* mengukur tingkat kompleksitas serangan yang dibutuhkan untuk mengeksploitasi kerentanan setelah penyerang memperoleh akses ke sistem target.
    a. *High*: kondisi akses khusus ada, seperti jendela waktu tertentu, konfigurasi jarang terlihat dalam praktek, atau metode *Social Engineering* yang akan dengan mudah digunakan untuk mendeteksi.
    b. *Medium*: kondisi akses Agak khusus ada, seperti konfigurasi non-default yang tidak umum digunakan atau metode *Social Engineering* yang kadang-kadang mungkin menipu pengguna.
    c. *Low*: kondisi akses khusus atau keadaan khusus tidak ada. Dengan kata lain, biasanya atau selalu dieksploitasi. Ini adalah kasus yang paling umum.
3. *Authentication measures (Au)* mengukur berapa kali penyerang harus otentikasi ke sistem target untuk mengeksploitasi kerentanan.
    a. *Multiple* : Dua atau lebih percobaan dari otentikasi yang diperlukan untuk mengeksploitasi kerentanan, bahkan jika tanda pengenal yang sama digunakan setiap waktu.
    b. *Single*: Salah satu contoh dari otentikasi yang diperlukan untuk mengeksploitasi kerentanan.
    c. *None*: Otentikasi tidak diperlukan untuk mengeksploitasi kerentanan.
4. *Confidentiality Impact (C)* mengukur dampak pada kerahasiaan jika kerentanan berhasil dieksploitasi pada system target.
    a. *None*: Tidak ada dampak pada kerahasiaan.
    b. *Partial*: pengungkapan informasi yang cukup.
    c. *Complete*: Semua informasi terbuka.
5. *Integrity Impact (I)* mengukur dampak pada integritas jika kerentanan berhasil dieksploitasi pada system target.
    a. *None*: Tidak ada dampak pada integritas.
    b. *Partial*: pelanggaran yang cukup dalam integritas.
    c. *Complete*: total kompromi terhadap integritas sistem.
6. Availability Impact (A) mengukur dampak pada ketersediaan jika kerentanan berhasil dieksploitasi pada system target
    a. *None*: Tidak ada dampak pada ketersediaan.
    b. *Partial*: Mengurangi kinerja atau interupsi dalam ketersediaan sumber daya.

c. *Complete*: mematikan seluruh sumber daya yang terpengaruh.

Proses pemberian nilai (scoring) pada base matric adalah sebagai berikut :

```
BaseScore = round_to_1_decimal(((0.6*Impact)+(0.4*Exploitability)-1.5)*f(Impact))
Impact = 10.41*(1-(1-ConfImpact)*(1-IntegImpact)*(1-AvailImpact))
Exploitability = 20* AccessVector*AccessComplexity*Authentication
f(impact)= 0 if Impact=0, 1.176 otherwise
AccessVector = case AccessVector of
   requires local access: 0.395
   adjacent network accessible: 0.646
   network accessible: 1.0
AccessComplexity = case AccessComplexity of
   high: 0.35
   medium: 0.61
   low: 0.71
Authentication = case Authentication of
   requires multiple instances of authentication: 0.45
   requires single instance of authentication: 0.56
   requires no authentication: 0.704
ConfImpact = case ConfidentialityImpact of
   none: 0.0
   partial: 0.275
   complete: 0.660
IntegImpact = case IntegrityImpact of
   none: 0.0
   partial: 0.275
   complete: 0.660
AvailImpact = case AvailabilityImpact of
   none: 0.0
   partial: 0.275
   complete: 0.660
```

Base score dihitung berdasarkan enam parameter yang telah disebutkan sebelumnya, setiap parameter telah ditentukan nilainya, impact dan exploitability terlebih dahulu. Selanjutnya kedua nilai tersebut dimasukkan ke dalam proses perhitungan base score. Berikut adalah contoh perhitungan base score :

```
Hasil penilaian : AV:N/AC:L/Au:N/C:N/I:N/A:C.
```

Maka diterjemahkan sebagai berikut :

```
BASE METRIC                    EVALUATION                          SCORE
-------------------------------------------------------------------------------
Access Vector                  [Network]                           (1.00)
Access Complexity              [Low]                               (0.71)
Authentication                 [None]                             (0.704)
Confidentiality Impact         [None]                              (0.00)
Integrity Impact               [None]                              (0.00)
Availability Impact            [Complete]                          (0.66)
```

Proses Perhitungan sebagai berikut :

```
BASE FORMULA                                                    BASE SCORE
-------------------------------------------------------------------------------
Impact = 10.41*(1-(1)*(1)*(0.34))                               == 6.9
Exploitability = 20*0.71*0.704*1                                == 10.0
f(Impact) = 1.176
BaseScore = (0.6*6.9 + 0.4*10.0 - 1.5)*1.176                    == 7.8
```

## 3. Metode Penelitian

### 3.1 Lokasi Penelitian

Tempat dan waktu penelitian dilakukan di STMIK STIKOM Bali dari bulan juni – Oktober 2015 dengan melakukan proses pengukuran pada jaringan internal salah satu jaringan internal STIKOM Bali.

### 3.2 Perancangan Penelitian

Dalam melakukan penelitian ini, penulis melakukan langkah-langkah penelitian sebagai berikut :

1. Studi awal
   Dalam melakukan studi awal, penulis melakukan : pencarian materi yang berkaitan dengan packet sniffing dan teknologi jaringan komputer.
2. Implementasi
   Pada tahapan ini, proses sniffing dimulai dengan menggunakan wireshark, dilanjutkan dengan mengelompokkan IP address dengan menggunakan network Miner
3. Penilaian Bussiness Impact Analisys
   Proses penilaian menggunakan IP yang dihasilkan dari network miner, dengan menggunakan perhitungan cvss version 2 dihasilkan bussiness impact analysis pada IP tersebut.

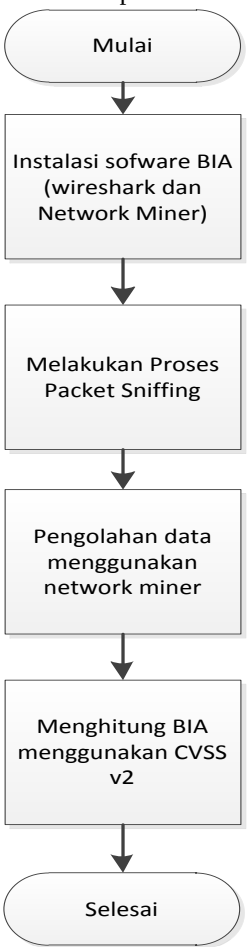
**3.3 Instrumen Penelitian**

Alat penelitian yang akan digunakan dalam penelitian dibagi dalam dua bagian utama yaitu perangkat lunak dan perangkat keras :

1. Perangkat Lunak
   - Perangkat lunak yang digunakan dalam penelitian ini adalah sebagai berikut:
   - Sistem Operasi Windows sevr
   - Aplikasi Wireshark
   - Aplikasi Network Miner
2. Perangkat Keras
   Perangkat keras yang digunakan dalam penelitian adalah komputer dengan spesifikasi processor Intel Core i3, 4 GB RAM, hardisk 160 GB, VGA 256 MB

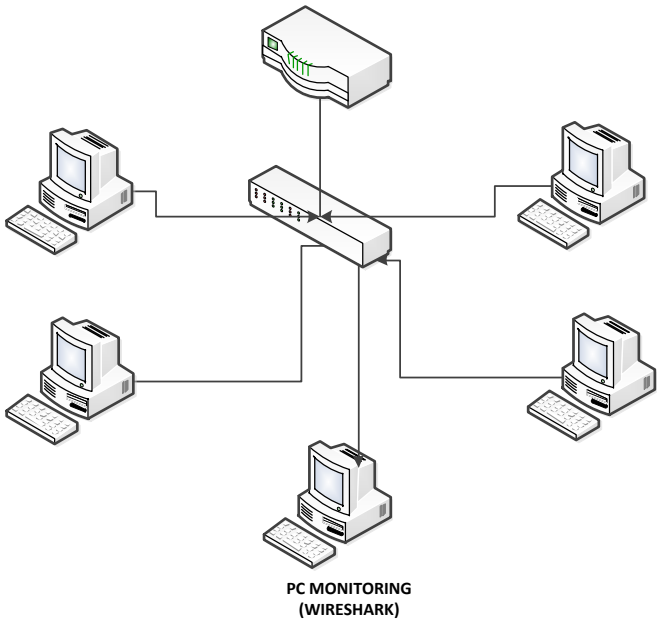
**3.4 Tahapan Pengumpulan Data**

Tahap pengumulan data dapat dilihat pada gambar 1. Proses Pengumpulan data. Proses pertama adalah melakukan iinstalasi dua peralatan yang digunakan menganalisa, dilanjutkan dengan melakukan proses sniffing di dalam jaringan STIKOM bali, dan proses terakhir adalha melakukan proses penglahan data sehingga bisa menjadi gambara bagaimana dampak bisnis dari penerapan teknologi yang digunakan.




*Gambar 1 Proses pengujian jaringan*

### 3.5 Arsitektur Jaringan




*Gambar 2. Arsitektur Jaringan*

Arsitektur jaringan yang digunakan dapat dilihat seperti gambar 2 arsitektur jaringan. Proses monitoring berada di dalam layer 2 disebuah jaringan lokal STIKOM Bali. Sehingga dengan demikian akan dapat dimonitoring apa saja data yang lewat melalui layer 2 tersebut. Teknik ini disebut SPAN. Dengan tujuan setiap paket data yang melewati layer 2 maka akan direkam di PC monitoring. Teknik ini adalah teknik sniffing yang paling mudah dan paling sering dilakukan. Semua komunikasi yang berada di sekitar perangkat tersebut atau menuju jaringan internet melalui jaringan tersebut akan direkam. Naik itu yang bersifat data terenkripsi maupun data plain text. Dari hasil tersebut nantinya pada pembahasan akan dibuatkan tabel mengenai komputer apa saja yang melakukan proses komunikasi dan resiko apa saja yang dihadapi dari teknologi yang digunakan.

## 4. Hasil dan Pembahasan

Dalam proses penentuan Bussiness Impact Analysis menggunakan teknik sniffing belum ditemukan standar baku. Namun dengan melakukan sedikit eksperimen, dapat diperoleh kerentanan pada traffic data yang memiliki potensi dampak keamanan jaringan. Hasil analisa dilakukan melalui langkah berikut ini :

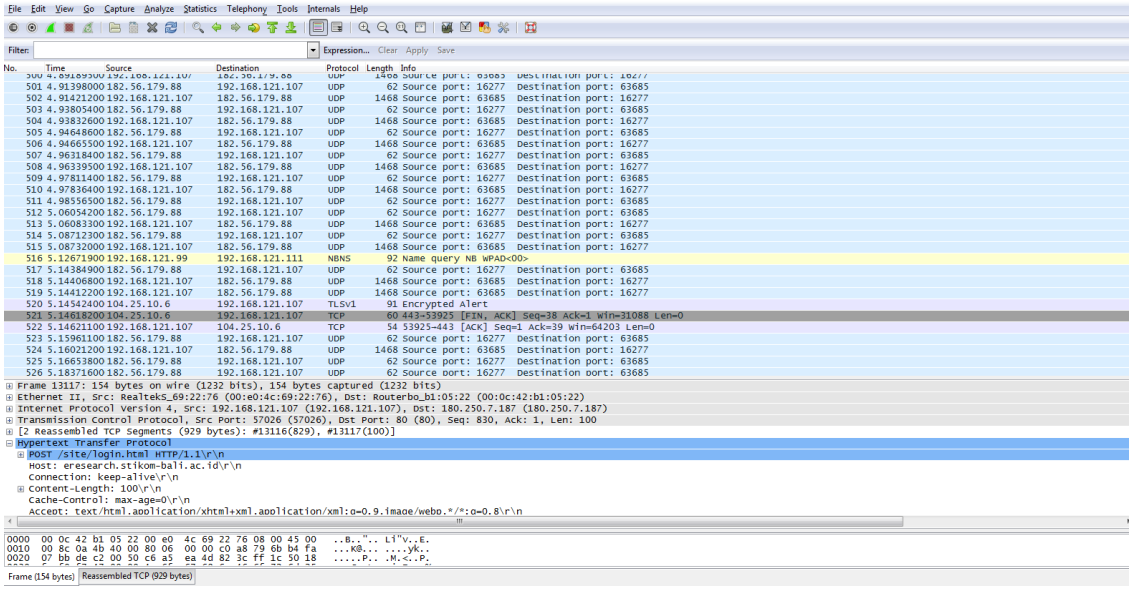
### 4.1 Proses Packet Sniffing

Proses paket sniffing dimulai dengan menjalankan proses capture packet di perangkat jaringan. Dengan memilih interface card yang akan digunakan untuk memonitoring traffic


*Gambar 3 Proses Memilih interface.*

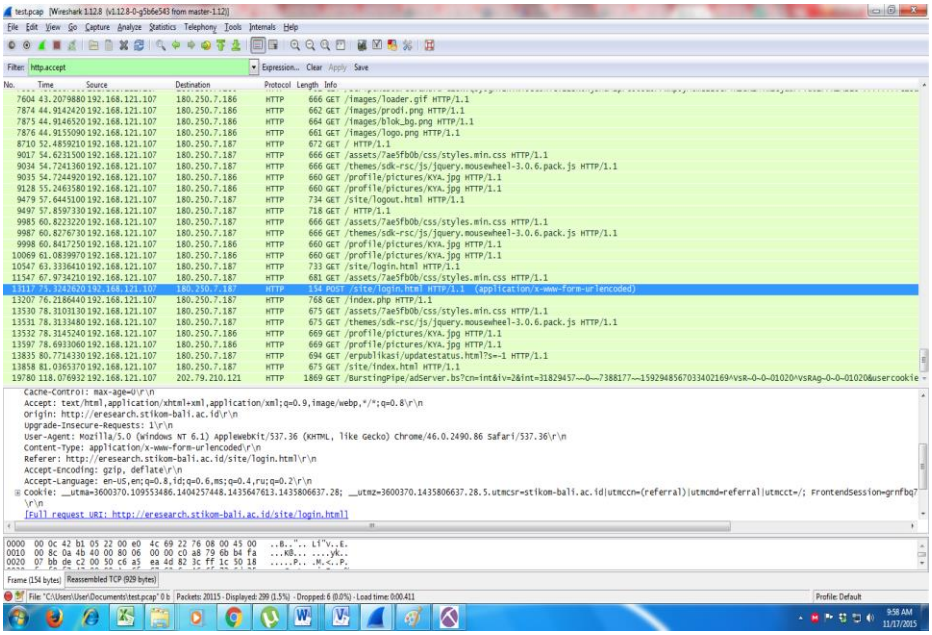
Gambar 3. Proses pemilihan interface memperlihatkan perangkat kartu jaringan mana yang akan dijadikan sebagai media untuk memonitoring jaringan. Untuk penelitian ini memilih dua kartu jaringan yang digunakan untuk melaukan proses capture traffic. Selanjutnya dilakukan proses untuk melakukan

sniffing dijaringan lokal. Proses sniffing dilakukan selama 1 jam di dalam jaringan lokal. Semua data yang lewat akan ditangkap oleh wireshark dan akan diolah dengan menggunakan fasilitas filter.
Dalam proses sniffing yang terlihat pada gambar 4 . selama satu jam didapatkan ribuan paket yang melewati jaringan lokal area network dan berbagai protokol seperti, TCP, UDP, ICMP, dan protokol yang lainnya. Dapat dilihat pada gambar traffic banyak menuju ke jaringan luar ataupun menuju ke jaringan internal. Paket yang dapat diambil atau di tangkap oleh wireshark berupa no, source ip address, destination IP address, protocol, panjang paket, dan yang terakhir info dari paket yang berhasil ditangkap.

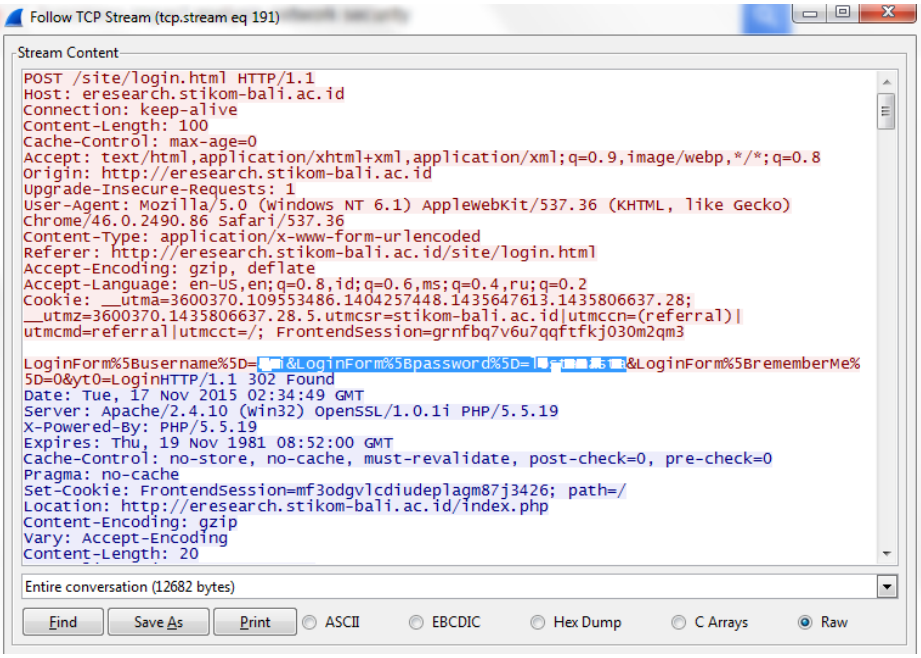


*Gambar 4 Sniffing menggunakan Wireshark*

Dari proses sniffing didapatkan ribuan paket yang melintasi layer 2 dari jaringan lokal area network. Sehingga dibutuhkan teknik filtering utuk mengetahui kerentanan yang ada di jaringan yang digunakan. Gambar 5. Penggunaan filter di wireshark menunjukkan salah satu filter untuk mengetahui kualitas jaringan. Beberapa filter yang digunakan adalah tujuannya untuk mengetahui resiko dari komunikasi yang menggunakan protokol HTTP. Dalam proses komunikasi di internet protocol ini adalah protokol yang sangat sering memiliki resiko yang besar, disamping protokol yang lain seperti TCP dan UDP.

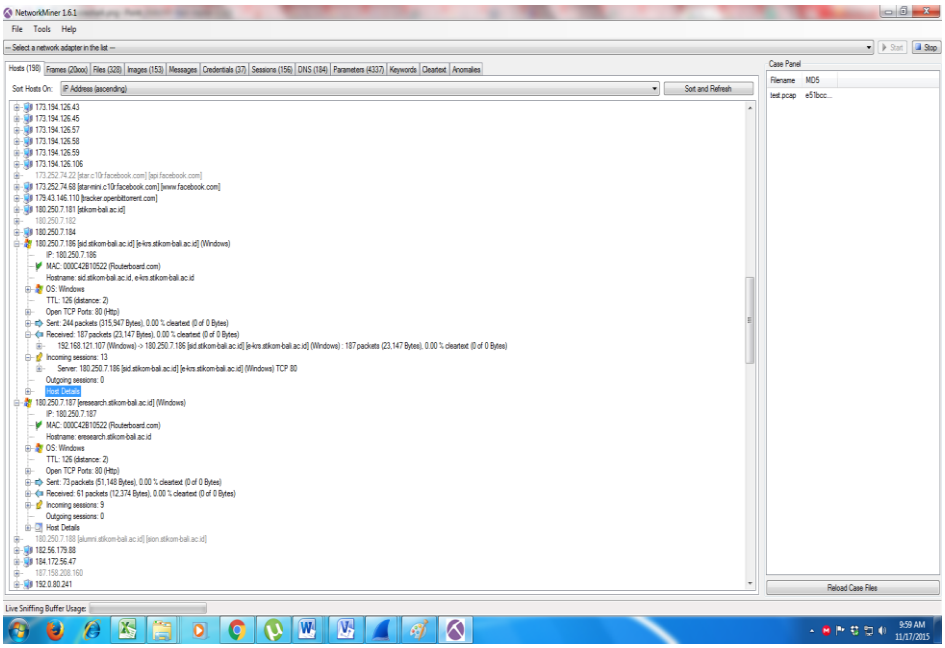


*Gambar 5 Penggunaan Filter di Wireshark*




*Gambar 6 Hasil Dari penerapan Filter*

Salah satu hasil yang tampak dari penerapan filter dapat dilihat pada gambar 6. Hasil dari penerapan filter. Traffic yang menggunakan protokol HTTP memiliki resiko terhadap bocornya data username dan password dari pengguna sehingga dapat menimbulkan dampak terhadap institusi jika sampai data account tersebut disalah gunakan oleh pihak yang tidak bertanggung jawab.



*Gambar 7 Mining IP Address Jaringan local Area Network*

Proses selanjutnya setelah resiko dan dampak sudah mulai terlihat adalah melakukan proses pengumpulan IP address yang melakukan transaksi. Dengan menggunakan aplikasi network miner maka akan terkumpul IP address berapa saja yang sedang melakukan komunikasi pada saat proses sniffing dan mengetahui bagaimana pola komunikasinya Gambar 7.

Setelah mendapatkan IP adress yang berkomunikasi, proses selanjutnya adalah memperhitungkan bussiness impact analysis berdasarkan kerentanan yang didapat dengan menggunakan perhitungan Commond Vulnerability Scoring System (CVSS) Version 2 untuk mengukur tingkat dampak

dari manajemen jaringan yang diterapkan. Dilihat pada gambar 7. Banyak IP address yang terlihat pada aplikasi network miner, namun dalam penelitian ini hanya mengambil ip address yang memiliki nilai High, Medium, dan low dalam proses komunikasi data.Didapatkan hasil bussiness impact analysisnya sebagai berikut :

| NO | *IP Adress* | AV | AC | Au | C | I | A | IS | ES | SC | LEVEL | PROTOKOL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 192.168.121.97 | 1.0 | 0.71 | 0.704 | 0.0 | 0.0 | 0.660 | 6.9 | 10 | 7.8 | *High* | HTTP, TCP, UDP |
| 2 | 192.168.121.99 | 1.0 | 0.71 | 0.704 | 0.0 | 0.0 | 0.660 | 6.9 | 10 | 7.8 | *High* | HTTP, TCP, UDP |
| 3 | 192.168.121.102 | 1.0 | 0.71 | 0.704 | 0.275 | 0.275 | 0.275 | 6.4 | 10 | 7.5 | *High* | HTTP, TCP, UDP |
| 4 | 192.168.121.104 | 1.0 | 0.71 | 0.704 | 0.275 | 0.275 | 0.275 | 6.4 | 10 | 7.5 | *High* | HTTP, TCP, UDP |
| 5 | 192.168.121.105 | 1.0 | 0.71 | 0.704 | 0.275 | 0.275 | 0.0 | 4.9 | 10 | 6.4 | *High* | HTTP, TCP, UDP |
| 6 | 192.168.121.107 | 1.0 | 0.71 | 0.704 | 0.275 | 0.275 | 0.0 | 4.9 | 10 | 6.4 | *High* | HTTP, TCP, UDP |
| 7 | 202.79.210.121 | 1.0 | 0.71 | 0.704 | 0.0 | 0.275 | 0.0 | 2.9 | 10 | 5 | *Medium* | HTTP, TCP, UDP |
| 8 | 203.190.241.2 | 1.0 | 0.71 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 10 | 5 | *Medium* | HTTP, TCP, UDP |
| 9 | 203.190.241.6 | 1.0 | 0.71 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 10 | 5 | *Medium* | HTTP, TCP, UDP |
| 10 | 203.190.241.9 | 1.0 | 0.61 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 8.6 | 4.3 | *Medium* | HTTP, TCP, UDP |
| 11 | 180.250.7.184 | 1.0 | 0.61 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 8.6 | 4.3 | *Medium* | HTTP, TCP, UDP |
| 12 | 180.250.7.186 | 1.0 | 0.61 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 8.6 | 4.3 | *Medium* | HTTP, TCP, UDP |
| 13 | 180.250.7.187 | 1.0 | 0.61 | 0.704 | 0.0 | 0.275 | 0.0 | 2.9 | 8.6 | 4.3 | *Medium* | HTTP, TCP, UDP |
| 14 | 182.56.179.88 | 1.0 | 0.61 | 0.704 | 0.275 | 0.0 | 0.0 | 2.9 | 8.6 | 4.3 | *Medium* | HTTP, TCP, UDP |
| 15 | 1876.158.208.160 | 1.0 | 0.35 | 0.704 | 0.275 | 0.275 | 0.0 | 4.9 | 4.9 | 4 | *Medium* | HTTP, TCP, UDP |

## 5. Kesimpulan

Kesimpulan dari penelitian Bussiness Impact Analysis Aplikasi Jaringan Komputer dengan teknik packet sniffing adalah sebagai berikut :

1. Telah berhasil dilakukan sniffing pada jaringan lokal menggunakan aplikasi wireshark
2. Dalam proses sniffing tersebut didapatkan ada 15 IP Address yang berkomunikasi
3. Dari ke 15 Ip address tersebut, dengan menggunakann metode penghitungan common vulnerability scoring system (CVSS) version 2. Didapatkan bussiness impact analysis berdasarkan vulnerability dari proses komunikasi data di jaringan dengan tingkat high sebanyak 6 dan jumlah medium sebanyak 9.

## Daftar Pustaka

[1] Noname. 2009. *Free Security Scanner For Network Exploration & Security Audits*. [online] available from : http://insecure.org [accessed 4 april 2011]

[2] William Lewis, Jr., Richard T. Watson, and Ann Pickren. 2003. *An Empirical Assessment of IT Disaster Risk.* didapatkan di http://paul-hadrien.info/backup/LSE/IS%20490/utile/assesment%20of%20disaster%20risk.pdf. [diunduh 4 oktober 2010].

[3] Raj Baral. 2010. *AASA a Protocol For Network Security Assessment Methodology.* Anglia Ruskin university, United kingdom. [diunduh 1 juli 2014]

[4] Abdul Latif, 2009, "Cara men-sniffing password menggunakan WireShark", didapatkan di http://blog.uad.ac.id/latif_ilkom/2009/10/19/cara-men-sniffing-password-menggunakan-wireshark/ [diakses 2 Juli 2011]

[5] Peter Mell, Karen Scarfone, Sasha Romanosky. *CVSS A Complete Guide to the Common Vulnerability Scoring System version 2.0*. National Institute of Standards and Technology and Carnegie Mellon University. July, 2007.